

STATE OF IDAHO

TELECOMMUTING POLICY

POLICY STATEMENT

It is the policy of the State of Idaho that state agencies who develop telecommuting programs must follow the guidance and instructions in this document prior to telecommuting implementation and must continue to adhere to those requirements during the duration of their program.

PURPOSE

This policy permits agencies to designate employees to work at alternate work locations for all or part of their workweek in order to promote general work efficiencies.

DEFINITIONS

Alternate Work Location	Approved work sites other than the employee's central workplace where official state business is performed. Such locations may include, but are not necessarily limited to, employees' homes or satellite offices
Central Workplace	An agency's place of work where employees normally are located
Resident Taxing State	The state where the employee is actually performing their assigned duties
Telecommuter	An employee who works away from his/her central workplace either at home or at another agency-designated or approved remote work location
Telecommuting	A work arrangement in which supervisors direct or permit employees to perform their usual job duties away from their central workplace, in accordance with work agreements
Work Agreement	The written agreement between the agency and employee that details the terms and conditions of an employee's work away from his or her central workplace. Work agreements are required for Telecommuting
Work Schedule	The employee's hours of work in the central workplace or in alternate work locations.

TELECOMMUTING

Telecommuting, also known as telework, is a mutually agreed upon workplace option between the agency and the employee, which allows work to be done by an employee at an alternate work location for one or more days each week. In most cases, some work will still be done at the employee's usual central workplace depending upon the needs of the agency. Telecommuting can be used by agencies to manage people, time, space, and workload more effectively and efficiently. When used properly, telecommuting programs can reduce commuting time and expenses for employees, improve recruitment and retention efforts, extend hours of customer service, improve employee performance and decrease overhead costs.

GENERAL REQUIREMENTS

1. Telecommuting Programs

As Telecommuting may not work for some agencies or employees, prior to developing a telecommuting program, agencies should consider their specific needs from a telecommuting program and which types of jobs are best suited for telecommuting and which ones may not be. It should also consider the types of employees and employee characteristics that are best suited to take advantage of these programs. Agencies should consider establishing a specified trial period to ensure that telecommuting will meet agency expectations.

2. **Agency Policy:** An agency that decides to implement a telecommuting program must adopt a written policy that defines the criteria and procedures for telecommuting and ensure that its agency-specific policy is consistent with this State policy. Additionally, the *State of Idaho's Guidelines for Telecommuting* will assist agencies in developing their telecommuting programs and procedures. Agency leadership is responsible for managing the affairs and operations of state government; thus, agencies have sole discretion to

- Designate positions for telecommuting
- Approve employees to telecommute

3. Resident Taxing State other than Idaho

All State of Idaho employees are expected to work within the State of Idaho. If an agency has a need for an employee (s) to work outside of the State of Idaho, the agency must first have approval from the Division of Financial Management and Division of Human Resources before hiring or allowing an existing employee to regularly perform their assigned duties from an out of state location.

Once the agency has received above approval, they must then notify the Idaho State Controller's 180 days in advance of paying the out of state employee. This advanced notice is required to allow for SCO system programming to correctly withhold payments required by the resident taxing state. The requesting agency will be billed for all associated programming costs.

In addition, the requesting agency will be responsible for processing of payments/reports and maintain all out of state accounts required by the resident state. This includes, but is not limited to:

- State tax withholding
- Worker's compensation
- Unemployment
- Wage reporting (W-2)

4. Telecommuting Agreement

An agency that develops a telecommuting program must develop a telecommuting agreement, attachment 1. This agreement must be signed by both the employee and the supervisor or appointing authority before telecommuting begins. A copy of this State policy and the agency's policy should be attached to the agreement or, at a minimum, cite the policies and ensure the employee has read and understands them. The sample agency agreement may be modified to fit the individual agency and employee circumstances. This agreement does not set forth additional rights for the employee nor establish a contract of employment where one otherwise does not exist.

Agency policies should address, at a minimum, the following conditions:

- The duration of the agreement.
- The work schedule and how it can be changed.
- How leave is to be requested and approved by the supervisor.
- The status of employees during emergency or weather-related closings affecting the central or alternate work location.
- How routine communications between the supervisor, employee, co-workers and customers will be handled.
- Any changes to the employee's performance plan and expectations because of telecommuting.
- The equipment and supplies that will be needed and who will be responsible for providing and maintaining them (see **6. Equipment and Materials** below).
- Applicable data security procedures (see **7. Security** below).
- Telecommuting location safety requirements.
- Requirement for employees to comply with all state and agency rules, policies, practices and instruction.
- Requirement that employees will notify their supervisor immediately of any situation which will interfere with their ability to perform their job.
- Have a statement that employees absolve the agency and the state from liability for damages to real or personal property resulting from participation in the telecommuting program.
- Provide consent by the employee allowing the agency access of the employee's alternate work site without prior notice.
- Provide for termination terms of telecommuting when requested by either the agency or the employee.
- Provide for the return of all state-owned equipment and supplies upon termination of the telecommuting period.

5. Conditions of Employment

Telecommuting assignments do not change the conditions of employment or required compliance with policies. An employee's compensation, benefits, and hours an employee is expected to work will not change as a result of telecommuting, regardless of the work location. Should the employee telecommute from outside the State of Idaho, a justification for telecommuting from outside the State of Idaho must be developed and any additional costs must be addressed in the Telecommuting Agreement. Typically, mileage or travel expenses to commuting to the regular work site will not be authorized. An employee telecommuting from outside the State of Idaho is subject to taxation in accordance with the state in which the alternate worksite is located. The State Controller's Office must be notified of this change. Agencies must ensure that procedures are in place to document the work hours of telecommuting employees and that individual work schedules are in compliance with the Fair Labor Standard's Act (FLSA).

Impact on work hours: Prior to implementing any telecommuting program, consideration should be given to how the program may impact an employee's weekly hours, leave and holiday schedules.

Overtime: Although exempt employees have inherent flexibility in scheduling and performing their work, non-exempt employees are covered by the requirements of the FLSA and therefore are subject to overtime pay for hours worked in excess of 40 hours in a week, or 160 hours in a 28-day period for employees designated as law enforcement.

Shift Differential: Shift differential pay will not be authorized for telecommuters even if the majority of work is performed between 6:00 p.m. and 6:00 a.m.

Holidays: Schedules resulting in holiday time off in excess of 8 hours should only be approved in such a way as to treat all members of the affected job classification equally. If flex schedules are in effect, they may be suspended, paid leave may be authorized, or work schedules may be adjusted during holiday weeks so as to ensure equity among all staff.

Mutual Agreement: Unless otherwise specified as a condition of the job at the time of hiring, the agency, the supervisor, and the employee must agree to telecommuting. Agencies are responsible for determining whether or not it is appropriate to offer telecommuting to any employee based on the agency's needs, policy, and the criteria normally applied to decisions regarding the approval of telecommuting.

Meetings: Supervisors may require employees to report to a central workplace as needed for work-related meetings or other events such as to discuss work progress, work assignment changes, etc. In general, business meetings or visits should not be held at an alternate work location when it is in a home. However, supervisors should have a reasonable expectation of occasional access to the alternate work location to perform supervisory duties. Mileage or travel expense reimbursement to and from the central work site will not be authorized.

Use of leave: Telecommuting is not intended to be used in place of sick leave, Family and Medical Leave, Workers' Compensation leave, or any other type of leave. However, agencies may decide to offer telecommuting as an opportunity for partial or full return to work based on agency, State and Federal policies and the criteria normally applied to decisions on telecommuting.

Non-Telecommuting Days: On a non-telecommuting day when the telecommuter is normally working at the central work place, including periods of severe weather or emergency closing, the telecommuting employee may not choose to work at the alternate work site and receive pay for work at the site unless supervisor approval is received in advance or prior to any work performed at the site.

Personal Business/Dual Employment: Employees may not be employed by another entity nor operate a personal business during the hours agreed upon as work hours. Further, Telecommuting employees shall not act as primary care givers for dependents or others nor perform other personal business during the hours agreed upon as work hours. If children or adults in need of primary care are in the alternate work location during an employee's work hours, some other individual must be present to provide care.

Operating costs: Agencies are not obligated to assume the responsibility for operating costs (utilities, phone, etc.), home maintenance, home office furniture, home office remodeling, or other costs incurred by employees in the use of their home as an alternate work location. It may be appropriate for agencies to pay for certain expenses such as cell phones, long distance work related calls on an employee's personal phone or other items that would otherwise be a normal operating expense for the agency.

Compliance: It is the employee's responsibility to ensure that they are in compliance with local zoning regulations if they are telecommuting from home. Telecommuters should be advised to contact their insurance agent and a tax consultant for information regarding alternate work locations in the home. The employee shall be responsible for tax and insurance consequences, if any, as a result of this arrangement.

6. Workers' Compensation & Injuries to Third Parties

The state's workers' compensation program provides coverage for injuries and illnesses incurred in the course and scope of employment. Therefore it is important that any telecommuting arrangement be clearly detailed in writing between the supervisor and employee so as to eliminate any chance of on-the-job injuries not being covered under workers' compensation.

Liability: In any telecommuting situation in which an employee works from their home, the employee remains liable for injuries to third persons and/or members of the employee's family occurring on the employee's premises.

7. Supervision

Any telecommuting option usually results in situations whereby a supervisor is not able to visually observe an employee's work performance. It therefore becomes important that not only are the right employees chosen for telecommuting programs,

but that supervisors develop appropriate and effective ways to supervise the work of those in a telecommuting program. To assist in measuring the success of the telecommuter in meeting performance standards, supervisors should focus on results generated by the telecommuter rather than on observed performance, and should also communicate in advance what assignments or tasks are appropriate and expected.

Supervisory impact: Supervisors will likely have to spend more time on some supervisory duties with telecommuters and communicate frequently to ensure the telecommuter is achieving their agency objectives. Supervisors must take care to communicate in advance what assignments or tasks are appropriate to be performed at the alternate work location, and what assessment techniques will be used to measure success in meeting performance standards.

Training: The agency may want to consider providing training to the managers, supervisors and employees who will be involved in telecommuting to ensure a complete understanding of the telecommuting agreement as well as to promote the best possible work accomplishments and employee relations.

8. Equipment and Materials

To ensure that appropriate security requirements are met and that work is being performed on equipment adequate for work requirements, the state agency must provide essential state-owned equipment to the telecommuter such as personal computers. To ensure ease of technical support and continued work efficiency at the central and alternative side, a laptop is recommended. The agency will determine who will provide additional equipment such as cell phones, printers, FAX machines, and other peripherals. If possible, agencies should consider using a “thin client” for the alternate work location since the absence of a hard drive would provide additional security to State information accessed at the alternate work location. (A ‘thin client’ is a computer with no disk drives and no data stored on it but connects to application and data servers that do the processing and store the data)

Authorized use: State-owned equipment is to be used for legitimate state business purposes, by authorized employees, and in conformance to ITRMC policy. The employee is responsible for protecting the state-owned equipment from theft, damage and unauthorized use.

Equipment installation and maintenance: Employees will be responsible for the transport of equipment and for returning it to the central workplace for maintenance and repair, as well as upon termination of the telecommuting period. The agency shall be responsible for maintaining, servicing and repairing all state-owned equipment and may provide assistance in the installation of equipment and software during normal work hours. The employee shall ensure no unauthorized software is installed on the state-owned computer. Agency-provided equipment (such as computers or cell phones) should be listed on the agency’s inland marine schedule if they wish to provide coverage for the equipment located at the alternate work site at a lower deductible. Otherwise, the equipment is covered by the State’s major property coverage and subject to a \$2,000 deductible.

Supplies: The agency shall provide the supplies and materials required for normal work activities related to the state-owned equipment. The employee will be responsible for transporting the materials to the alternate work location unless otherwise agreed to in their Telecommuting Agreement.

Internet connection: In most cases, the employee will be responsible for providing a high speed Internet connection if electronic access is required from their home to the state's network, as well as any additional phone lines if needed. An agency may consider this to be a normal expense and reimburse the employee for all or a portion of the costs.

Home office: If the alternate work location is in the home, the work location furniture and space shall be provided by the telecommuter. If a locking file cabinet is required for the protection of data and work documents, it should normally be provided by the employee.

9. Security

Telecommuting from home presents security risks that the employee and the State must mitigate to ensure the confidentiality, integrity and availability of State information and network services. For those employees that work with sensitive information such as HIPAA, it is unlikely that a home environment will meet the protection needs, so agencies must carefully consider if these employees should become telecommuters.

Protection of Information: All State information, regardless of sensitivity level, must be protected. Adequate precautions must be taken at the telecommuter location to ensure the security of State data, hardware and communication links. Employees will adhere to all agency approved security Policies, Standards and Guidelines to ensure confidentiality, integrity and availability of State resources. State data, applications, documents and other state resources must be protected by the telecommuter from unauthorized viewing, use or access by all third parties including family and friends. In the event a telecommuter has received authorization from agency management to transport or store sensitive data at their alternate work location, data encryption and/or physical security measures must be implemented.

Screen-lock: Telecommuters must utilize a screen-lock program on the computer used for work at the alternate work location. Furthermore, to ensure their computer is locked and the information and network is secure, they must have a minimum screen-lock time of 20 minutes. Employees must be instructed on how to use the screen-lock program.

Encryption: Windows has built in file and folder encryption capabilities and official state information should be encrypted using at least this technology. Agencies should consider investing in commercially available, 128-bit to 256-bit AES or 3DES disk encryption technologies. For those agencies that process data which requires Federal Information Processing Standards of Protection, to include privacy data, and want to use Windows Encryption, they must use the 3DES encryption option.

Physical protection: The agency must decide what level of physical protection is required for the information a telecommuter works on. The protection, at a minimum, must match the security required for that information in the central workplace. Agencies should consider using “thin-client” technology to minimize the possibility of any information breaches at the alternate work location.

Protection in Transit: Telecommuters should ensure they protect State information and information technology, such as computers, hard drives, and removable media between the central workplace and the alternate work location. Telecommuters must avoid leaving the equipment or documents in a car, even if it is locked. If State equipment and/or documents must be left in an automobile, they must be locked in a hard trunk.

Wireless Networks: Telecommuters should not access the network using a home wireless network unless strong security features are enabled, to include 128-bit to 256-bit AES or 3DES encryption of the wireless signal. All wireless network access that is not being used must be turned off.

Incident Reporting: The agency must establish an incident reporting process in case of a security incident or an information breach. State standards apply and are available at <http://www2.state.id.us/itrmc/plan&policies/Policies> to help the agency create a process. All telecommuters must be trained on this reporting process.

Supervisory awareness: Supervisors must be aware of what information is at the telecommuter’s alternate work location. While the employee may have access to the agency’s resources through remote access, the employee must ensure the supervisor is aware of what documents and data the employee is accessing.

Patching and maintenance: Telecommuters must only use State-owned computer equipment and protective software used by the agency in order to meet State IT security standards. The responsible agency must ensure security patching and anti-virus updates are maintained on the telecommuter’s hardware (PC, PDA, etc). If at all possible, the agency should accomplish this patching via the Virtual Private Network (VPN) In addition; the responsible agency will determine how they will resolve computer maintenance issues and user assistance.

Standards Compliance: Electronic access by telecommuters to all internal resources, applications, data and services on the state’s network and at agency locations must be made according to the established state’s Virtual Private Network (VPN) standard (S3220). Employees must ensure that no unauthorized people, to include friends and family, have access to the State equipment, data or VPN connection. The VPN technology used must initiate a security check for current security patches, anti-virus/anti-spyware signatures and a firewall.